AMD PENSANDO

WHITE PAPER | CASE STUDY

ATOS SUPERCHARGES NETWORKING AND SECURITY PERFORMANCE WITH VMWARE VSPHERE® AND AMD PENSANDO™ DPUS

March 2024

VMware Horizon®
Virtual Desktop Use Case
Proof of Concept

Technical Summary

In 2022, VMware® launched vSphere® 8, featuring the capability to offload infrastructure services to a data processing unit (DPU) like the one at the heart of the AMD Pensando™ Distributed Services Card (DSC). This joint innovation brings a number of benefits and value to every server that is DPU-enabled. First, “bare-metal-like” performance drives exceptional throughput and lower latency for networking and security functions required for modern and data-driven applications. Second, overall security posture is increased by 1) leveraging distributed firewall (DFW) for microsegmentation on all workload interfaces, and 2) by separating VM and hypervisor security control application attack vectors (now running isolated on the DPU).

At the same time, offloading and acceleration via the DPU enables additional efficiencies—high VM density per node, robust power efficiency across clusters, low TCO, and enhanced energy efficiency for new deployments. By reducing the overall required compute footprint, organizations can significantly reduce power consumption and related CO_2 emissions. VMware has integrated DPUs directly into the existing vCenter® and VMware API architecture, so consumption at large scale is seamless and simple from an operations viewpoint.

ATOS SUPERCHARGES NETWORKING AND SECURITY PERFORMANCE WITH VMWARE VSPHERE® AND AMD PENSANDO™ DPUS

Overview

With the release of vSphere 8 and NSX® 4, VMware has added support for data processing units (DPUs)[1]. With the DPU functionality in vSphere, called *vSphere Distributed Service Engine*, core infrastructure services like networking, security, and storage can be offloaded to the DPU from the x86 host's hypervisor. Currently, networking (routing, switching) and security (firewall), along with operations/monitoring are offloaded to the DPU. In conjunction with vSphere 8, NSX-T 4 and Uniform Pass Through (UPTv2) with the AMD Pensando DPU, customers can fully realize the benefits of hypervisor bypass (or hardware passthrough) without the typical limitations of SR-IOV—specifically removing the inability to support critical vSphere features such as vMotion and DRS. UPTv2 functionality is supported with the rest of the NSX networking and advanced security stack, including distributed firewall (DFW) and IDS/IPS functionality. This allows the platform to provide improved application performance (leveraging the best throughput and latency, because it's passthrough) with all the networking and security features (L4 DFW for microsegmentation) enabled and supported for any application/workload.

[1] originally referred to by VMware as "SmartNICs"

ATOS SUPERCHARGES NETWORKING AND SECURITY PERFORMANCE WITH VMWARE VSPHERE® AND AMD PENSANDO™ DPUS

This document highlights key learnings from an evaluation conducted by Atos of VMware vSphere® on DPUs, combined with VMware Horizon® as the virtual desktop solution, running all required workload and management infrastructure on modern OEM systems (Dell and HPE) backed by AMD DPUs.

Atos Background and Use Case

Atos is a global leader in digital transformation with 105,000 employees. European number one in cyber security, cloud and high-performance computing, Atos provides tailored end-to-end solutions for all industries in 69 countries. Atos is a pioneer in decarbonized digital for its clients. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, Atos enables its customers and employees, and members of societies at large, to live, work and develop sustainably, in a safe and secure information space.

As a digitization partner, Atos aids clients by being a leader in cloud and digital. Atos is also ranked #1 in managed security services worldwide by revenue (2021). With these capabilities and technical excellence, Atos cloud services will greatly benefit from the best-in-class performance, increased security protection, and more efficient use of computing power (kWh) provided by DPUs.

Atos currently uses several products from VMware's portfolio to power their infrastructure and architecture, including VMware vSphere®, VMware NSX®, and VMware Horizon®. This enables Atos to operate various high-performance VDI environments, in addition to some SDDC (software-defined data center) environments containing mission critical workloads, where performance and security are top of mind and some of the highest priority metrics for their solution offerings.

Proof of Concept: Physical Topology

The POC tested the first generation of DPU-enabled servers from Dell: the PowerEdge R750 with dual Intel Xeon® Gold 5320 CPUs running 26 physical cores at 2.2 GHz and 256 GB of DDR4 memory. The servers have a standard NIC interface for out-of-band ESXi™ management, but for testing, Atos leveraged the 100 Gb/s AMD Pensando DPU connected to a low-latency top of rack switch (ToR) to evaluate offloading performance and benefits. The compute infrastructure was hosted in an isolated AMD DPU Test Drive environment, and the cluster included a dedicated vCenter and NSX manager.

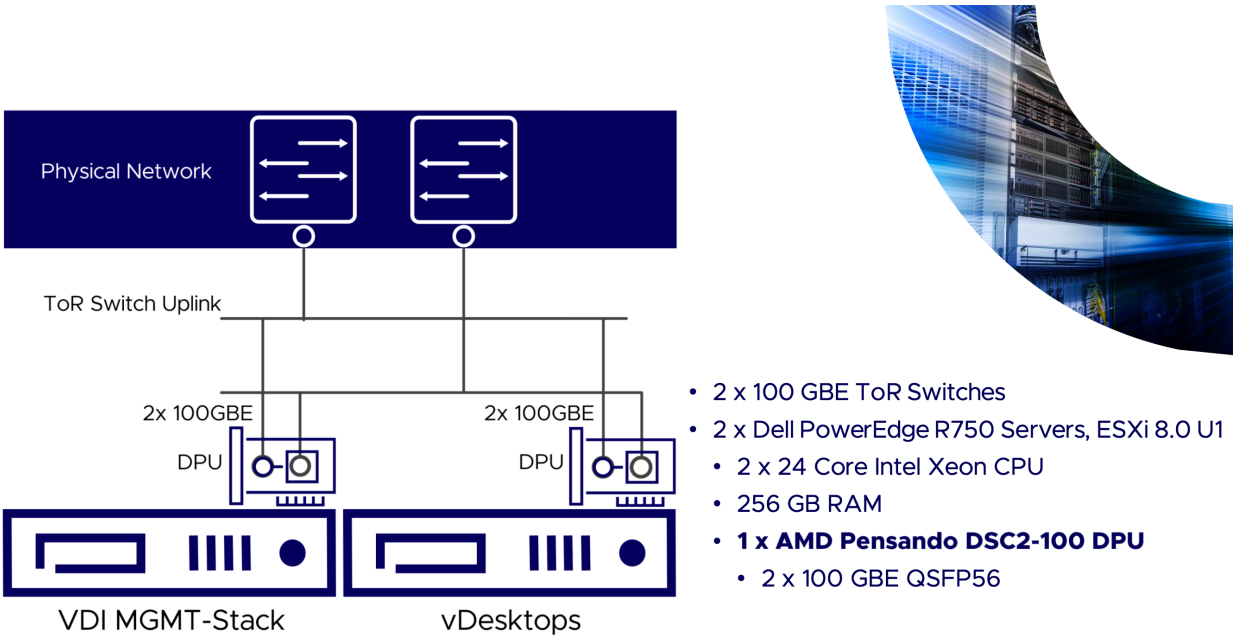

Figure 1. Proof of concept architecture: hardware infrastructure

Testing Methodology

Across all testing scenarios, three modes were leveraged during the proof of concept (POC):

- **Baseline** (Enhanced Data Path Standard): this represents what Atos would measure and observe with a comparable standard NIC (such as a ConnectX-6 100 Gb/s Ethernet adapter), using ESXi and NSX functions on the x86 host
- **DPU Emulated Mode** (Enhanced Data Path Standard): this represents the DPU default mode where a large portion of the networking and security processing is offloaded to the DPU
- **DPU Full Acceleration Mode** (Enhanced Data Path Standard with UPTv2): this represents having most of the networking and security processing offloaded to the DPU, while observing the passthrough or “bare metal”- like performance while maintaining core vSphere functions such as HA, DRS, and vMotion support

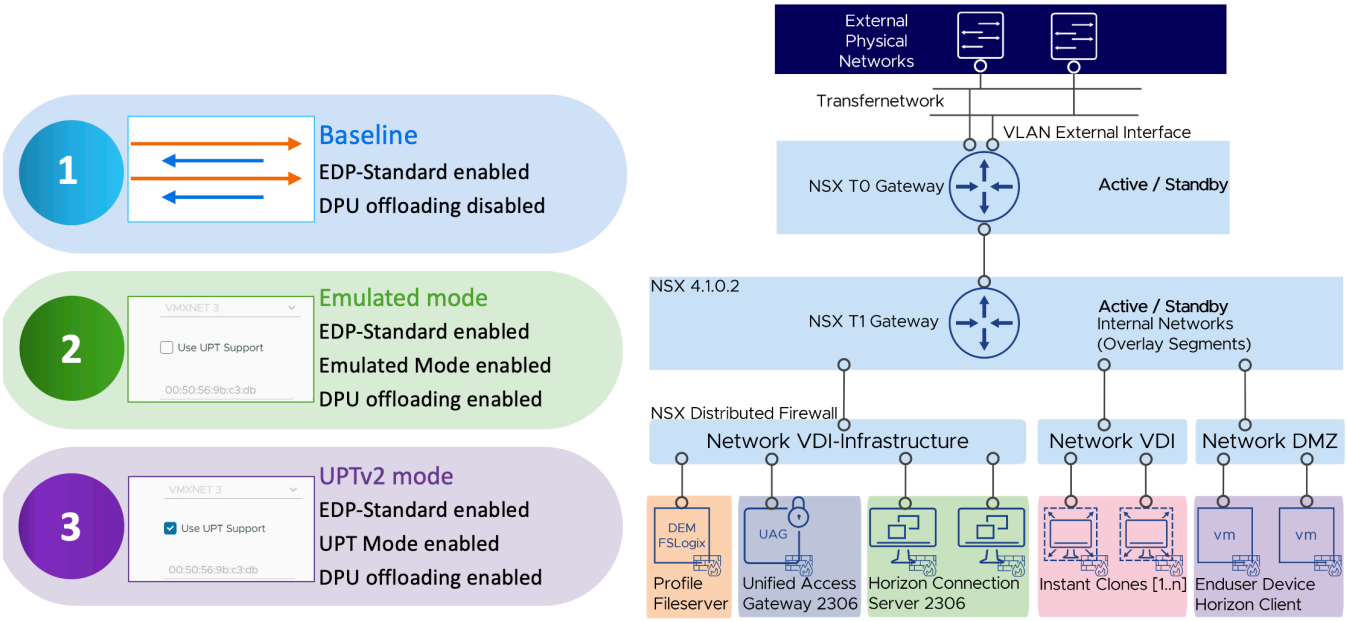

Figure 2. Proof of concept architecture: logical infrastructure, testing methodology

Testing, Observations, and Results

The first test performed was designed to evaluate end-user experience. Atos wanted to determine if there would be any impact to a user's logon duration when leveraging DPUs in their compute platforms—specifically, measuring the time between double-clicking in the Horizon client to login and the point where the user is presented with and logged into their Windows® desktop environment.

The first step was to create a VDI master image with typical elements such as a Windows 10 image and additional components as shown in Figure 3:

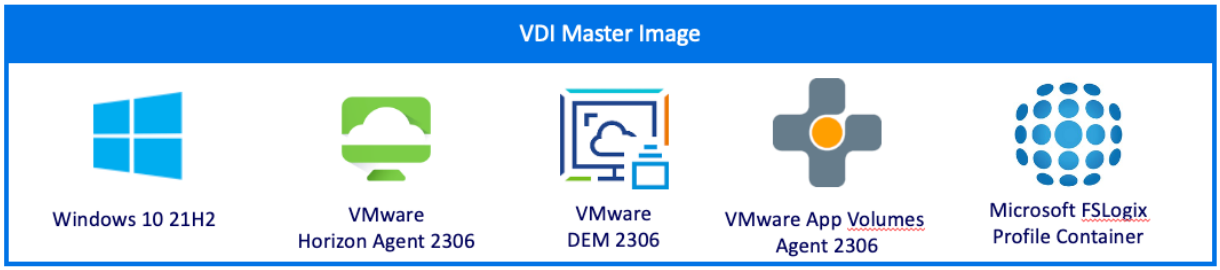

Figure 3. Specified elements for testing VDI login duration

In the test, Atos cloned 20 instant clones to the ESXi node exclusively for virtual desktops, and ran a load generator in those desktops to push about 50% CPU usage on the host ESXi node to simulate a production load scenario.

The results of this test are shown in Figure 4. The baseline testing showed about 15 second login time; the emulated mode and UPT results were quite a bit faster. The login times were split into different segments to observe and understand exactly where the improvements are throughout the entire login process.

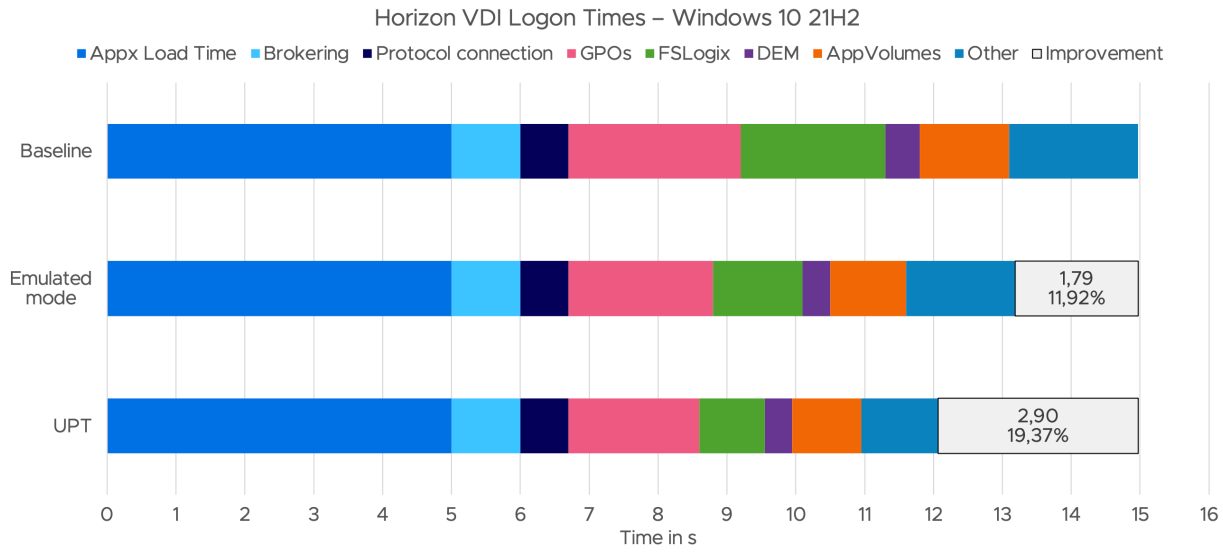

Figure 4. Testing VDI logon duration

A closer look at the results reveals that there is no change to the Appx Load time. This is to be expected since this is an internal Windows process, and does not touch the network at all, so there is no opportunity for network acceleration. Similarly, the second

and third metrics—Brokering and Protocol connection—are Horizon-specific processes and again no change was observed.

The next four metrics are where things get interesting, as these processes all showed a reduction in login time. Using DPUs has accelerated the communication between the virtual desktops and the management stack; each of these areas has had a decrease in their login time compared to the original baseline.

In summary, Atos observed ~12% decrease in login duration for emulated mode, and ~20% reduction when the desktops and management VMs were configured with UPT mode.

The second test evaluated desktop density, to see if leveraging DPUs in compute nodes can allow Atos to increase their VM density. There is an inherent CPU core savings, given that the network and security functions are now offloaded to the DPU and not consuming x86 cores. Atos wanted to run as many desktops as possible on the VDI server, but it should be noted that this test was limited to the physical server configurations available in the POC lab. The density could be much higher, and these results would predictably be even better if the physical server contained Atos' production server configuration (essentially more CPU cores per socket and higher DIMM/memory density).

Given these hardware restraints, the baseline configuration was 20 virtual desktop hosts. The load generation tool in this test is the *Fish Tank* benchmark, which generates images and motion pictures to put all desktops under load.

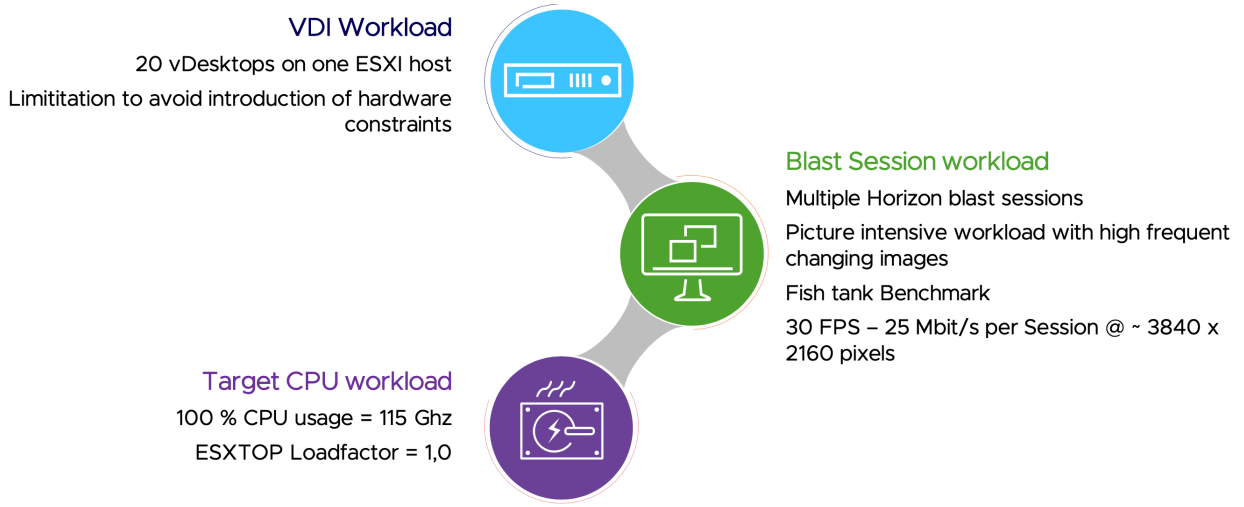

Figure 5. Setup for measuring density improvements due to DPUs

The results of this test are shown in Figure 6. The summary data shows an approximate 8% density increase in virtual desktops with emulated mode, and a 17% improvement in virtual desktops with UPT mode. To understand how Atos was able to get 17% more virtual desktops, the right-hand chart shows the number of CPU cores consumed when ESXi is processing networking (overlay networks) and security (distributed firewall). This shows the total number of CPU cores consumed to process the network packets. In UPT mode, where network functions are offloaded to the DPU, and there is near zero point zero CPU utilization on the x86 side, which allows Atos to increase the scale and density of the virtual desktops, given that those cores are not being consumed by network I/O.

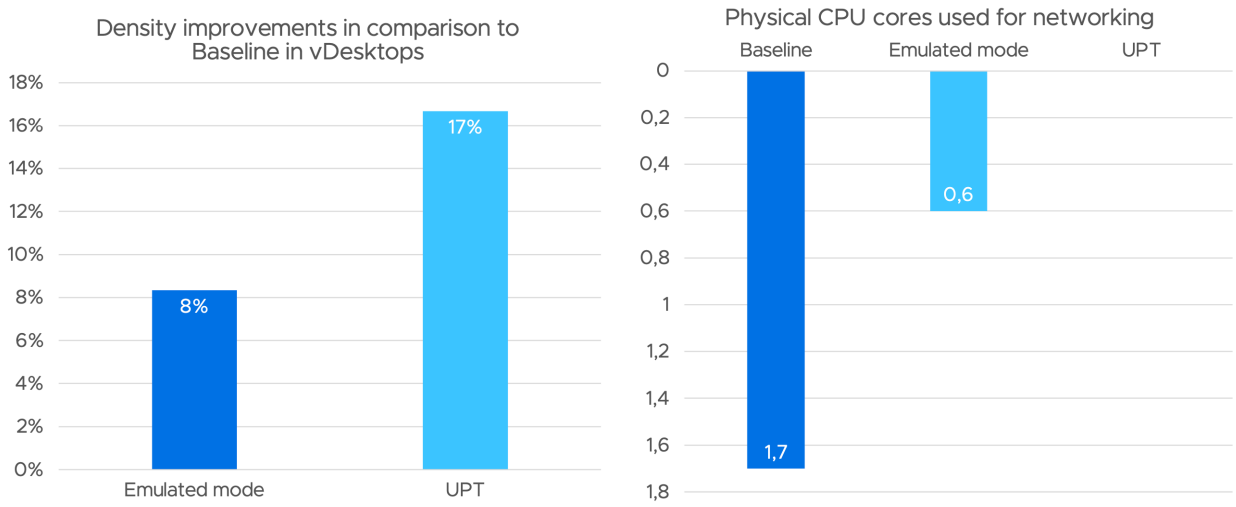

Figure 6. Density improvement results

A tertiary benefit observed during the density testing was in network throughput for the desktops. During density testing, the *iperf3* benchmark was used as a network load simulator. In the baseline test, the benchmark showed roughly 26.6 Gb/s of traffic; using the exact same parameters, there was an 8% throughput increase to the baseline number with emulated mode, and a 46% increase when the VMs were configured with UPT mode.

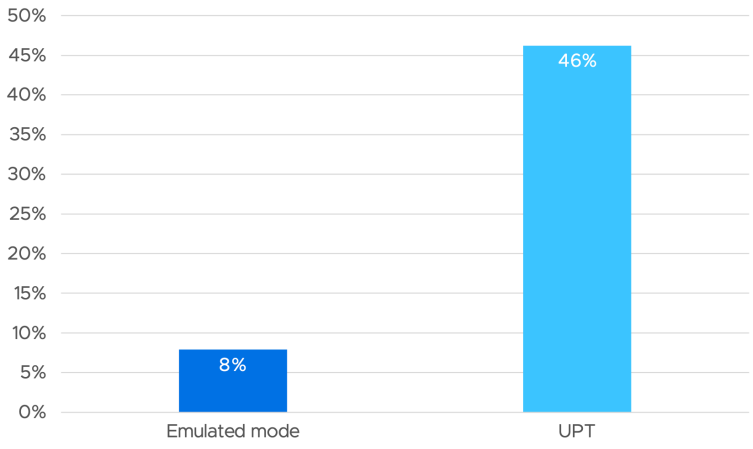

Figure 7. Network throughput increases (iperf3), compared to a baseline of 26.6 Gb/s

Another benefit observed was not related to performance. Any organization in today's modern service or hosting provider business will always have a keen eye on how they can leverage and improve their security posture. Many modern attacks and breaches are a result of the "land and expand" methodology, where an attacker leverages a vulnerability and gains access to a trusted system. From there, bad actors can exploit that vulnerability to gain privileged access to the virtual machine, or even worse, the hypervisor layer itself, and then disable or kill any type of network security controls, giving them freedom to move within the host or across the network with nothing to stop the attack from spreading. The DPU architecture fundamentally changes all of this.

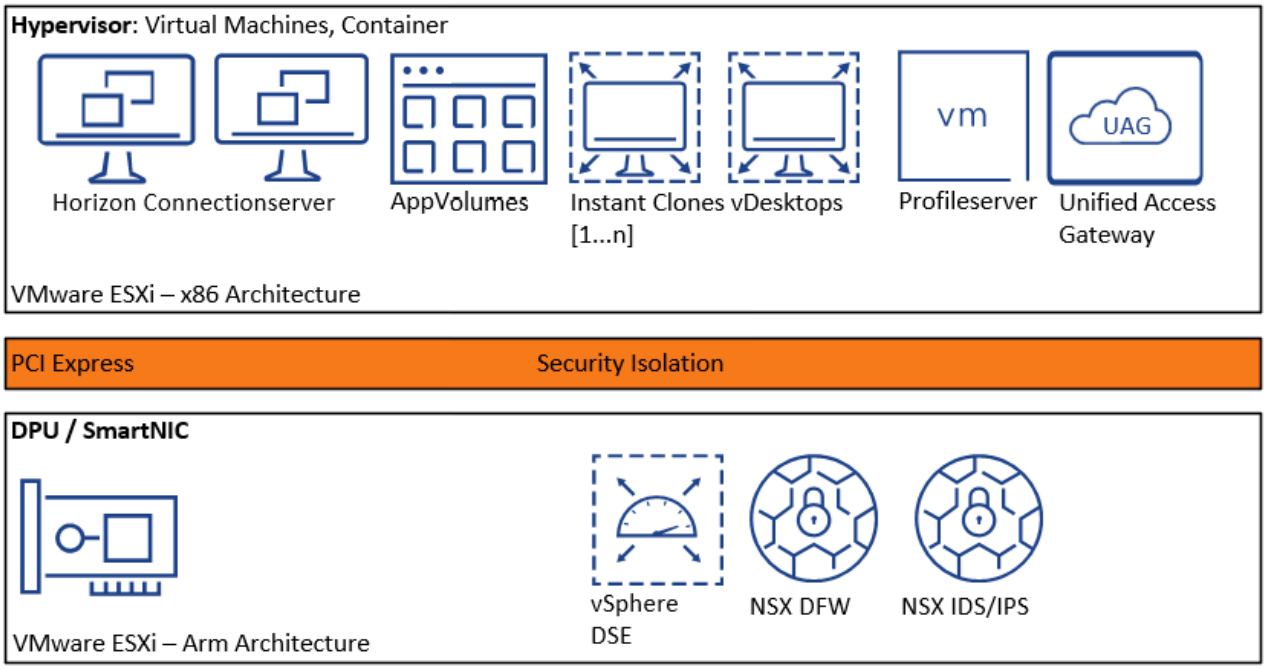

Figure 8. Enhancing security by offloading functions to the DPU

Figure 8 is an example of Atos' VDI environment today, where all the critical components run on the ESXi instance on the x86 host. When Atos introduced the DPU into their architecture, this added a physical separation between the ESXi instance running in x86 and the ESXi instance running on the DPU's CPU complex. This moves the NSX functions, or more generically the networking and security pieces, from x86 to this isolated instance running on the DPU, providing an additional layer of security isolation between where the applications and desktops run and where the security and access controls are running and executed.

Figure 9 shows a hypothetical example where an Atos VDI user may have been phished, and their desktop has succumbed to a speculative execution vulnerability, but the DPU and the network and security controls remain unimpacted. This is because of the security isolation on the PCI Express® bus and the fact that the NSX software and functions are running in an isolated ESXi instance on the DPU, such that the security controls for the rest of the architecture remain in place and limit what the malicious user can do and access.

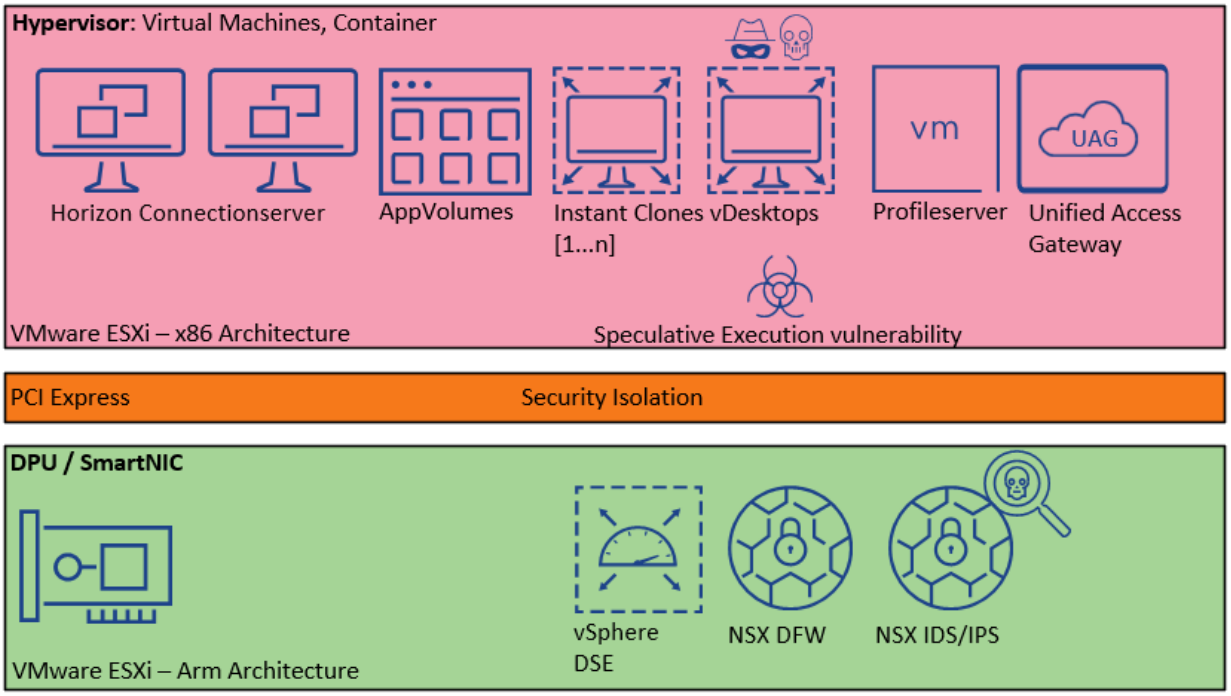

Figure 9. Example security threat: compute hypervisor

Summary

The Atos performance tests show a very impressive result in accelerating networking performance while freeing up CPU resources on the physical ESXi servers. With the capabilities offered by the vSphere Distributed Services Engine and the AMD Pensando DPU, Atos was able to validate exceptional performance for their VDI environments moving forward. In addition, simply adding the DPU into their compute nodes reduced certain attack vectors for their clients and customers. In addition, given some of the density measurements observed, Atos will be able to offer more vDesktops per physical node, which over time will allow them to build infrastructure to provide the same level of scale but with a reduced footprint, which will continue to allow them to address data center sustainability initiatives, as well as lower their overall project costs by requiring less physical infrastructure (which can result in benefits including less power consumption, less rack space, fewer physical servers, fewer switch ports, and lower licensing costs).

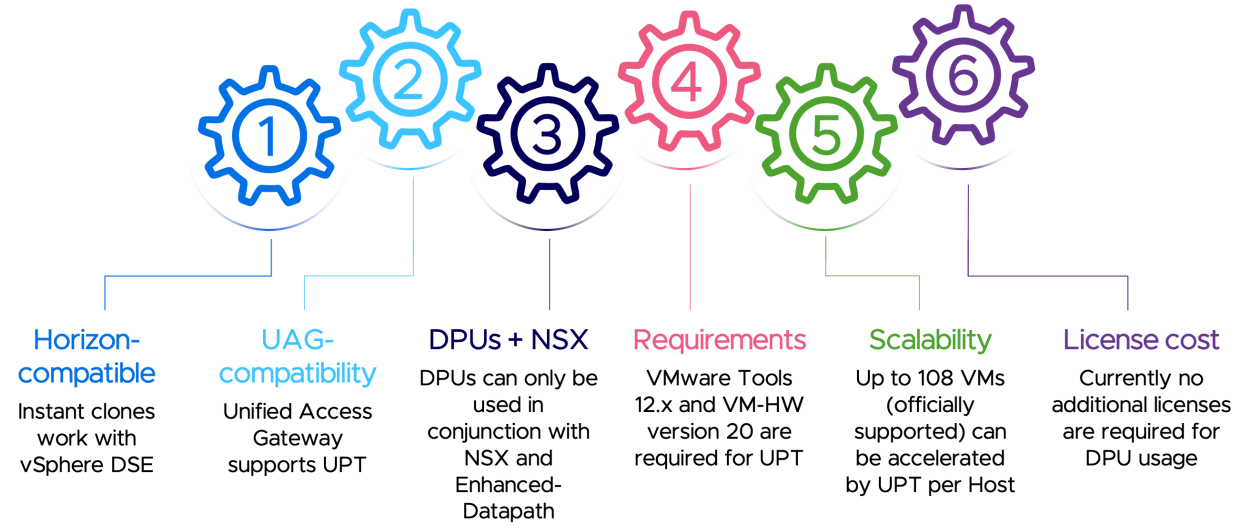

Figure 10. Key takeaways (Note: VMware officially supports a maximum of 108 VMs.)

Learn More

vSphere on DPUs

- VMware product page

Atos and Their Evaluation of AMD Pensando DPUs

- Atos Group web site
- VMware Explore 2023 breakout: Supercharge Your VDI Workloads: Unleashing the Power of SmartNICs

AMD Pensando DPUs; Take a Technology Test Drive

- AMD Pensando DPUs product page
  - Hands-On Lab: AMD Pensando™ DPU Test Drive for VMware vDSE

AMD
together we advance_virtualization

Disclaimer

All performance and/or cost savings claims are provided by Atos and have not been independently verified by AMD. Performance and cost benefits are impacted by a variety of variables. Results herein are specific to Atos and may not be typical. GD-181.

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. The information contained herein is subject to change and may be rendered inaccurate for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product releases, product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

THIS INFORMATION IS PROVIDED 'AS IS." AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS, OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION. AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY RELIANCE, DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AMD, the AMD Arrow logo, EPYC, Pensando and combinations thereof are trademarks of Advanced Micro Devices, Inc. Arm® is the registered trademark of Arm Limited in the EU and other countries. PCIe® is a trademark of PCI-SIG Corporation. VMware® is a trademark of Broadcom. Xeon® is a trademark of Intel Corporation or its subsidiaries. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

© 2024 Advanced Micro Devices, Inc. All Rights Reserved.

amd.com/pensando

PWP24003